UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,460	12/23/2003	Su Hyung Jo	122988-05007274	8145

43569 7590 02/01/2007
MAYER, BROWN, ROWE & MAW LLP
1909 K STREET, N.W.
WASHINGTON, DC 20006

EXAMINER	
SCHMIDT, KARI L	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/743,460	JO ET AL.	
	Examiner	Art Unit	
	Kari L. Schmidt	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *23 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 15-16 are rejected under 35 U.S.C. 101 because "recording medium" is directed to non-statutory subject matter. The recording medium may be signals, software, and a piece of paper and, which are not statutory.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Antoine, Vanessa. Router Security Configuration Guide. National Security Agency: http://www.securityfocus.com/infocus/1728: September 27, 2002.

Claim 1

Antoine discloses a security engine management apparatus in network nodes comprising: a security engine including: a security instruction and library subsystem for processing every application program and utility that are allowed to access to a system source; a policy decision subsystem for determining a filtering policy, an intrusion

detection policy and an access control policy that are required for detecting and blocking an intrusion into a network; an authentication and access control subsystem for preventing an unauthorized user from using a system and allowing an authorized user to access to the system in response to an application of the access control policy (Section 3.4.4 and Section 4.3); a policy application subsystem for analyzing and applying the policies (section 4.3.1); a packet filtering subsystem for receiving an allowed packet and denying a disallowed packet in response to the application of the filtering policy (Section 3.2.2); and an intrusion analysis and audit trail subsystem for analyzing and coping with the intrusion into the network in response to the application of the intrusion detection policy (page 229), and a security management subsystem for managing the security engine (Section 3.4.2).

Claim 2

Antoine discloses the security engine management apparatus in network nodes of claim 1, wherein the policy application subsystem provides intrusion detection and audit information (page 45 and 126:"audit logs") through a device driver and packet statistical information (page 41) through a proc file system to the policy decision system.

Claim 3

Antoine discloses the security engine management apparatus in network nodes of claim 1, wherein the filtering policy is used for blocking or passing a packet having a certain destination address depending on a sender address, a destination address, a sender port, a destination port, and a protocol type (Section 4.3.1 and Section 3.2.2, page 36 & 81).

Claim 4

Antoine discloses the security engine management apparatus in network nodes of claim 1, wherein the intrusion detection policy includes rules for detecting a DoS attack and a specific virus pattern (Section 5.5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 5 -16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Antoine, Vanessa. Router Security Configuration Guide. National Security Agency: http://www.securityfocus.com/infocus/1728: September 27, 2002. in view of Cuff, Andy. Intrusion Detection Terminology (Part One). http://www.securityfocus.com/infocus/1728: September 9, 2003.

Antoine discloses a security engine management apparatus in network nodes comprising: a security engine including: a security instruction and library subsystem for processing every application program and utility that are allowed to access to a system source; a policy decision subsystem for determining a filtering policy, an intrusion detection policy and an access control policy that are required for detecting and blocking an intrusion into a network; an authentication and access control subsystem for preventing an unauthorized user from using a system and allowing an authorized user to access to the system in response to an application of the access control policy (Section 3.4.4 and Section 4.3); a policy application subsystem for analyzing and applying the policies (section 4.3.1); a packet filtering subsystem for receiving an allowed packet and denying a disallowed packet in response to the application of the filtering policy (Section 3.2.2); and an intrusion analysis and audit trail subsystem for analyzing and coping with the intrusion into the network in response to the application of the intrusion detection policy (page 229), and a security management subsystem for managing the security engine (Section 3.4.2).

Antoine discloses the security engine management apparatus in network nodes wherein the policy application subsystem provides intrusion detection and audit information (page 45 and 126:"audit logs") through a device driver and packet statistical information (page 41) through a proc file system to the policy decision system. The filtering policy is used for blocking or passing a packet having a certain destination address depending on a sender address, a destination address, a sender port, a destination port, and a protocol type (Section 4.3.1 and Section 3.2.2, page 36 & 81).

The security engine management apparatus in network nodes wherein the intrusion detection policy includes rules for detecting a DoS attack and a specific virus pattern (Section 5.5.1). In case the virus file is downloaded, the intrusion analysis and audit trail subsystem detects the virus file transfer by examining a file pattern and then informs the virus file transfer on a mobile terminal; and in case the DoS attack is attempted, the intrusion analysis and audit trail subsystem examines a DoS attack pattern to block the DoS attack, thereby storing detection information on the DoS attack and the virus attack in an audit recording database (Section 5.5).

Antoine discloses the security engine management apparatus in network nodes wherein the network setting module displays network interface information on an interface card type, an IP address, a hardware address, and a size, state and option of maximum transmission unit (MTU), and system information on OS information, a booting elapsed time, a current time, a system name, and a disc size, and performs an addition, a deletion, and an edition of a routing table (Section 4.4 and pages 153-157).

Also Antoine discloses a method for security engine management in network nodes, comprising the steps of: (a) receiving a packet from an attack system and examining the packet according to a filtering policy; (b) checking whether the packet is allowed or not, based on the examination result of step (a); (c) passing the packet if the packet is allowed in the step (b) and checking whether or not the allowed packet is an attack intrusion packet according to an intrusion detection policy; and (Section 3.2.2) (d) in case the packet is the attack intrusion packet in the step (c). The security engine management method in network nodes wherein if the packet is disallowed in the step

(b), the disallowed packet is denied (Section 3.2.2). The security engine management method in network nodes of in which if the packet is a general packet in the step (c), the packet is transferred through a network (section 3.2.2). Includes a recording medium for recording therein a program for implementing a method for security engine management (page 24 & 66).

Furthermore Antoine discloses a method for providing an integrative security management by using a security policy applied between a router and a security management subsystem, the method comprising the steps of: (a) checking whether or not a user is authorized through a user registration and authentication process; (b) if the user is authorized in step (a), allowing a user to access to the security management subsystem, collecting information on a network composition of hosts, gateways, and routers and storing the collected information in a network database (Section 3.4.3-3.4.4). Wherein if the user is not authorized in the step (a), the user is blocked to access to the security management subsystem and system sources of network nodes to prevent damage generated by an illegal acquisition of a root authority (page 100: "preventing unauthorized access to resources on the network"). And if the user is not authorized in the step (a), a security engine is managed based on a security policy and the security policy is stored in a policy database (page 164: "Authorization works by creating a list of attributes which describe what the user is allowed to do. After a user logs in and has been identified by authentication, the security server database will be used to control access to various network components and services as defined by the stored attributes (if the user is authorized or not)"). Includes a recording medium

for recording therein a program for implementing a method for providing an integrative security management (page 43 & 127).

Antoine doesn't specifically state that security engine management apparatus or the methods use a security management GUI or a mobile terminal to communicate with a system operator when displaying statistical information on packet filtering or information on DoS and virus attacks.

Cuff discloses the security engine management apparatus, method for security engine management and method for providing an integrative security management in network nodes wherein the security management subsystem further includes: a security management GUI of a web base, for executing a management instruction; an audit management module for processing audit information on an illegal intrusion; a log-in processing module for performing a user authentication by using a user ID and a password inputted from the mobile terminal; a packet statistical module for showing packet statistical information on each of protocols and an interface; a network setting module for showing a network status for routers and systems through the security management GUI; a policy management module for displaying a security policy for detecting a network intrusion and performing an addition, a deletion, and an edition thereof; an audit management module for displaying information on the DoS attack and the virus attack on the mobile terminal by using a short message service (SMS); and a network communication module for communicating with the policy decision subsystem for a policy management and informing the audit management module of the policies in

real time (page 1: "alerts using GUI or mobile phone (SMS: "text messages") when the system operator detects suspicious activity").

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Antoine by using a GUI to display statistical information and also alert DoS attacks and virus attacks through a mobile terminal, which is disclosed in Wheeler. Using a GUI makes it easier for humans to read the activity that is going on with the security engine management apparatus and when the network is under attack and need to alert the system operator quickly using text messaging of a mobile terminal is beneficial.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Kaashoek et al. teaches a method of thwarting denial of service attacks on a victim data center coupled to a network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday-Friday: 7:30am - 5:00pm (with alternate Fridays off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER